REMARKS

Claims 1-28 and 33-34 are pending in the present application. Claims 1, 4, 7, 10, 13, 17, 21 and 25 are independent claims. Claim 33 is presently amended.

35 U.S.C. 112, 1st Paragraph

Claims 33 and 34 stand rejected under 35 U.S.C. 112, 1st paragraph for failing to satisfy the written description requirement. Applicant respectfully traverses this rejection.

With respect to claim 33, Applicant has replaced the reference to "OSI standard" with "IP communications standard", as Applicant acknowledges that the IP suite model is not necessarily mapped to 7 model layers in OSI (although they can be). Applicant submits that there are numerous references to IP protocols in the present application, as well as to examples of the claimed "transport layer" (e.g., UDP or TDP, see [0056]). Thus, Applicant has provided an adequate written description for the newly recited claim language.

Claim 34 was added to reinforce Applicant's arguments submitted in Applicant's previous response, where the Examiner was intending to read certain claims upon a file storage security protocol (with the file being a "higher-layer data object", such as an application layer where files are typically manipulated). This was intended to contrast with transport or packet layer encryption protocols. In other words, encryption applied to data packets can be performed without taking into account the entirety of the file from which the individual packets were partitioned for transport. Applicant believes that the language of claim 34 is consistent with this interpretation of the claims, and further that the Specification provides written description support for embodiments wherein encryption is performed without regard to "a higher-layer data

object" (e.g., see [0260]-[0262], where the user can selectively encrypt all traffic without regard to particular files, etc., because it is performed at a layer lower than the application layer).

Applicant respectfully requests that the Examiner withdraw this rejection.

35 U.S.C. 103(a) Alden in view of Citta

Claims 1, 4, 7, 13-28 33 and 34 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Alden in view of Citta. Applicant respectfully traverses this art grounds of rejection.

Discussion of Alden

As discussed in the previous Office Action, Alden is directed to a pseudo network adapter for frame capture, encapsulation and encryption. The general functionality of Alden's pseudo network adapter is discussed with respect to Figure 15, as follows:

> During operation of the elements shown in FIG. 15, the pseudo network adapter 259 registers with the network layer in the TCP/IP stack 260 that it is able to reach the IP addresses of nodes within the virtual private network 249 as shown in FIG. 14. For example, the pseudo network adapter on the client system registers that it can reach the pseudo network adapter on the server. Subsequently, a message from the tunnel client addressed to a node reachable through the virtual private network will be passed by the TCP/IP stack to the pseudo network adapter 259. The pseudo network adapter 259 then encrypts the message, and encapsulates the message into a tunnel data frame. The pseudo network adapter 259 then passes the tunnel data frame back to the TCP/IP protocol stack 260 to be sent through to the physical network adapter in the tunnel server. The tunnel server passes the received data frame to the pseudo network adapter in the server, which de-encapsulates and decrypts the message.
>
> *(Emphasis added) (See Column 14, line 58 to Column 15, line 8 of Alden)*

As will be appreciated from a review of the above-excerpt of Alden, the pseudo network adapter 259 (i) receives a message or packet, (ii) encrypts the packet, (iii) encapsulates the encrypted packet within a data frame for transmission, (iv) transmits the data frame to another pseudo network adapter where the data frame is de-encapsulated and decrypted.

The pseudo network adapter of Alden can only apply the same encryption to all packets

The pseudo network adapter 259 of Alden appears to apply the same level and type of encryption to all packets. Alden states "[t]pseudo network adapter 259 then encrypts the message, and encapsulates the message into a tunnel data frame" (See Column 14, line 58 to Column 15, line 8 of Alden). Nothing in this section indicates, for example, "encrypting a first data frame based on a first unique code" and "encrypting a second data frame based on a second unique code" as recited in claim 1.

With regard to the "encrypting a second data frame based on a second unique code" limitation, the Examiner cites to the same section of Alden as the "encrypting a first data frame based on a first unique code" limitation; namely, column 3, lines 18-19 of Alden (See Page 3-4 of the Office Action). This section states "[t]he transmit path includes an encryption engine for encrypting the data packets and an encapsulation engine for encapsulating the encrypted data packets into tunnel data frames" (column 3, lines 18-19 of Alden). Nothing in this section teaches "encrypting a first data frame based on a ***first*** unique code" and "encrypting a second data frame based on a ***second*** unique code" as recited in claim 1 (emphasis added).

Alden also fails to disclose anything related to sequential code encryption

Further, Applicant agrees with the Examiner in that Alden fails to "disclose that the encryption is based on sequential code encryption" (See Page 5 of the Office Action). However, the Examiner alleges that Citta discloses this particular deficiency of Alden.

Discussion of Citta

Citta is directed to a secure data packet transmission system and method. Citta teaches the transmission of a global bit packet encrypted with a global encryption key followed

sequentially by individually addressed packets (i.e., intended for a subset of subscribers, and not a global broadcast) encrypted with address keys. Thus, the global packets can be data associated with a free television broadcast, and the individually addressed packets can be for a pay-per-view (PPV) television broadcast, or premium channel such as HBO, Showtime, etc.

Citta discloses a data encryption and error protection (DEEP) feature, which is a software tool that performs encryption and error correction on packets (Column 2, line 54-61 of Citta). With regard to DEEP, Citta states that "[m]emory 30 is for storing the address and address key for the particular subscriber terminal. The address and address keys are permanent and 'burned into' the memory at the factory" (Column 4, lines 60-65 of Citta). Thus, the subscriber terminals store the (i) address and (ii) address keys internally and permanently. The (i) address is used to determine what type of content is being received at the subscriber terminal (e.g., HBO, Showtime, etc.), and the (ii) address keys are used to decrypt that content at the subscriber terminal (also, predetermined session keys are used to decrypt global packets, e.g., see column 5, lines 4-15 of Citta).

Packet decryption of global/individual packets at the subscriber terminal is discussed in detail in the following section of Citta:

> With particular reference to the flow chart [of FIG. 4], initially a counter in the subscriber terminal is reset to zero. The previously used session key is loaded into the subscriber terminal DEEP shift register, the start code is detected and the resulting CRC code (i.e. the 16 bit remainder of the processed packet) for the global packet is checked. If the CRC code matches (remainder of all zeros), it is presumed that the session key is correct and that there are no errors in the data. At that point, the counter is reset to zero and the global packet is processed for any general information therein, that is, information that is applicable to all subscriber terminals. Next the terminal address key is loaded into the DEEP shift register for processing the first received addressed data packet. Again the CRC is checked. If the CRC code is not all zeros, the packet either is addressed to a different subscriber terminal or there are errors in it. In either event, the packet is ignored. If the CRC code shows all zeros, an address comparison is made in the subscriber terminal controller to see if indeed the packet is meant for that subscriber terminal. If the address comparison shows a mismatch, the packet is ignored. If the address comparison shows a match, the packet is processed by the microprocessor and

> the procedure is repeated for the next two addressed packets. It is thus seen that the microprocessor only processes packets that are intended for it.
>
> *(Column 6, lines 21-47 of Citta)*

As will be appreciated from the above-excerpt of Citta, the subscriber terminal first checks whether a previously used session key (i.e., session keys are for global packets only) decrypts the global packet without errors (if errors present, packet is ignored). Next, because the global and individual packets are always sent in the same order, the subscriber terminal's address key is next used to decrypt each subsequent/sequential individual packet. If errors are present, the subscriber terminal ignores the packet; otherwise, if the CRC code indicates no errors, the subscriber terminal has sufficient authorization to decode the packet (e.g., to watch HBO, a PPV boxing match, etc.).

Neither Alden nor Citta teach including a code from which a unique encryption code is derived in a data frame

As an example, independent claim 1 recites "encrypting a first data frame based on a first unique code … said first unique code being *derived from a first sequential code*" and "encapsulating said first encrypted data frame in a first transport frame, *said first transport frame comprising a first portion and a second portion of said first sequential code*" (Emphasis added). A similar recitation is directed to the second data frame, with respect to different unique/sequential codes.

As discussed above, Alden discloses nothing related to applying different encryption to different data frames. Citta *does* disclose applying different encryption to different data packets (i.e., global packets vs. individual subscriber packets). However, both Alden and Citta fail to disclose or suggest deriving a unique encryption code based on a sequential code, using the unique encryption code to encrypt a data frame and then encapsulating the sequential code

within the data frame. The only components of the data frame in Citta are 48 data bits (i.e., content) and the 16 CRC bits used to determine whether authorization is sufficient (e.g., "each packet consists of 48 bits of 'data' and 16 bits of CRC code" at Column 3, lines 49-51 of Citta). Likewise, no code used to establish the encryption key in Alden is added to the data frame by the pseudo network adapter 259. The Examiner alleges that Alden discloses this limitation at Column 3, lines 19-21, but Alden merely discloses a general encapsulation of tunnel data frames in this section, and is silent regarding what is comprised within the tunnel data frames here.

Again, as recited in claim 1, the data frame is encapsulated so as to include a sequential code used to derive a unique key, which is then used to encrypt the data frame. No such bundling of different sequential codes is present within the transmitted data frames in Alden or Citta.

In view of the above remarks, Applicant respectfully submits that the combination of Alden and Citta fail to disclose or suggest "encrypting a first data frame based on a first unique code … said first unique code being *derived from a first sequential code*" and "encapsulating said first encrypted data frame in a first transport frame, *said first transport frame comprising a first portion and a second portion of said first sequential code*" (Emphasis added) as recited in independent claim 1 and similarly recited in independent claims 4, 7, 10, 13, 17, 21 and 25.

As such, claims 14-16, 18-20, 22-24, 26-28 and 33-34, dependent upon independent claims 1, 13, 17, 21 and 25, respectively, are likewise allowable over Alden in view of Citta at least for the reasons expressed above with respect to independent claims 1, 13, 17, 21 and 25, respectively.

Applicant respectfully requests that the Examiner withdraw this art grounds of rejection.

35 U.S.C. 103(a) Alden in view of Citta and further in view of Perlman

Claims 2, 5, 8 and 11 stand rejected under 35 USC § 103(a) as being unpatentable over Alden in view of Citta and further in view of Perlman (US 6363480). Applicant respectfully traverses this art grounds of rejection.

Initially, Applicant agrees with the Examiner regarding the failure of Alden and Citta in disclosing or anticipating certain claim limitations present within claims 2, 5, 8 and 11. The Examiner alleges, however, that Perlman discloses these particular claim limitations.

Perlman is directed to a method of ephemeral decryptability. A review of Perlman indicates that Perlman fails to cure the suggestion and disclosure deficiencies of Alden in view of Citta related to independent claims 1, 4, 7 and 10. As such, claims 2, 5, 8 and 11, dependent upon independent claims 1, 4, 7 and 10, are likewise allowable over Alden in view of Citta and further in view of Perlman at least for the reasons given above with respect to independent claims 1, 4, 7 and 10.

Applicant respectfully requests that the Examiner withdraw this art grounds of rejection.

35 U.S.C. 103(a) Alden in view of Citta and further in view of Semper

Claims 3, 6, 9 and 12 stand rejected under 35 USC § 103(a) as being unpatentable over Aldre in view of Citta and further in view of Semper. Applicant respectfully traverses this art grounds of rejection.

Initially, Applicant agrees with the Examiner regarding the failure of Alden and Citta in disclosing or anticipating certain claim limitations present within claims 3, 6, 9 and 12. The Examiner alleges, however, that Semper discloses these particular claim limitations.

Semper is directed to a system and method providing backward compatibility of radio link protocols in a wireless network. A review of Semper indicates that Semper fails to cure the

suggestion and disclosure deficiencies of Alden in view of Citta related to independent claims 1, 4, 7 and 10. As such, claims 3, 6, 9 and 12, dependent upon independent claims 1, 4, 7 and 10, are likewise allowable over Alden in view of Citta and further in view of Semper at least for the reasons given above with respect to independent claims 1, 4, 7 and 10.

Applicant respectfully requests that the Examiner withdraw this art grounds of rejection.

Reconsideration and issuance of the present application is respectfully requested.

Conclusion

In light of the amendments contained herein, Applicants submit that the application is in condition for allowance, for which early action is requested.

Please charge any fees or overpayments that may be due with this response to Deposit Account No. 17-0026.

Respectfully submitted,

Dated: April 10, 2008

By: /Raphael Freiwirth, Reg # 52,918/

Raphael Freiwirth
Reg. No. 52,918
(858) 651-0777

QUALCOMM Incorporated
Attn: Patent Department
5775 Morehouse Drive
San Diego, California 92121-1714
Telephone: (858) 658-5787
Facsimile: (858) 658-2502